

SECRET - KEY

DISTINGUISHER

GOAL: distinguish between
a Pseudo-Random Permutations
(PRP) and a cipher instantiated
with a secret key.

Ingredients:
- Cipher (Enc_k, Dec_k)
- PRP

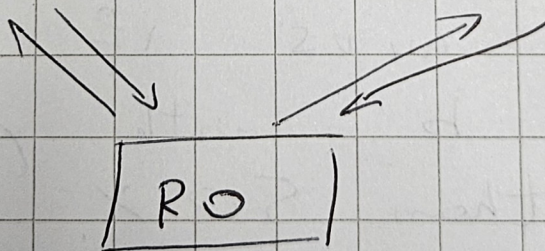
Game

if $b = 0$

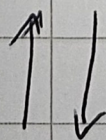
$\boxed{\begin{array}{l} Enc_k(\cdot), \\ Dec_k(\cdot) \end{array}}$

if $b = 1$

$\boxed{\begin{array}{l} PRP, \\ PRP^{-1} \end{array}}$



m (or
 c)



corresponding
 c (or m)

① Challenger chooses at random
 $k \leftarrow \{0, 1\}^k$ and PRP

(kept secret)

② Challenger picks up $b \xleftarrow{\$} \{0, 1\}$
random

IF $b = 0$: RANDOM ORACLE (RO)
instantiated with cipher

IF $b = 1$: RANDOM ORACLE
instantiated with PRP

③ Adversary queries RO with
→ messages / plaintexts m
and gets back ciphertext c
→ ciphertexts c and gets
back messages m

Adversary wins if he can
identify b with probability
higher than 50%.